

Postrehy zo SIEM projektov

eFOCUS

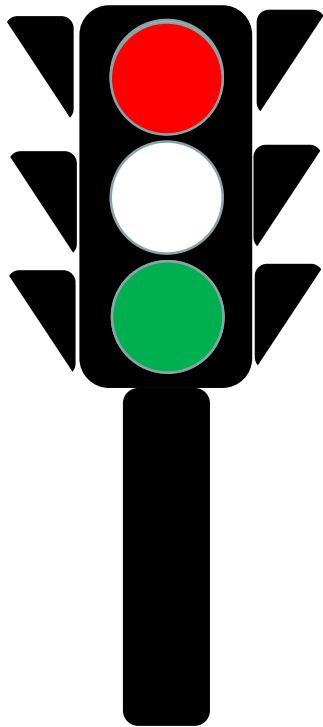
LYNX[®]

Postrehy zo SIEM projektov

Gabriel Benko CISSP, LYNX - spol. s r.o. Košice



Zákazník vs. dodávateľ



Otázky a odpovede

Základné otázky

**Je všetko
v poriadku?**

Čo sa deje?

Predpoklady pre odpovede

Mat' informácie o dianí

Rozumieť informáciám

Poznať normálne správanie

**Vedieť rozpoznať
a analyzovať anomáliu**

Niektoré výzvy ...a možné odpovede

Útočník

**Vyberá si čas,
miesto a spôsob**



Nedovoliť mu to:

- obmedzenia na autentizáciu, povolené operácie
- eliminovať možné cesty
- využiť výhodu domáceho ihriska- honeypoty

**Množstvo
potencionálnych
útočníkov
vs.
Limitované
kapacity ITSec**



Včasné podchytenie rizikových subjektov:

- identifikácia rizikových skupín a jednotlivcov
- identifikácia a monitorovanie rizikových tendencií
- monitorovanie aj tolerovaných odchýliek



**Zameriavanie sa na rizikové subjekty
počas rutinného monitoringu**



**Zníženie skupiny možných rizikových
subjektov:**

- awareness
- deterrence-výkon monitorovania, riešenie incidentov

Začíname

- Analýza
 - IT infraštruktúra, alebo čo tu všetko máme?
 - Výber zdrojov hlásení pre monitorovanie
 - Ktorý SIEM?
- Implementácia SIEM nástroja
 - Core časť
 - Konfigurácia auditných nastavení na zdrojových systémoch
 - Pripájanie zdrojov hlásení

Logy máme v SIEM, ale čo sa deje?

- Normalizácia, kategorizácia

zabezpečí SIEM, alebo mu pomôžeme?

- Poznám svoju infraštruktúru?

include SIEM into change management

OR

use custom tools

- Ako odlíšiť normálne správanie od anomálie?

Toto tu nebolo, to naozaj, tadiaľ ide komunikácia ?!

Nutná kooperácia s IT operation

Baseline

Trendy, Data monitory, Pattern Discovery

Rozhodnutie o incidente

**Nejednoznačné
dôkazy**

**Nízka výpovedná
hodnota
informácií**

**Nedostatok
informácií**

**Hrozba krivého
obvinenia**



Mat' rýchlo maximum informácií:

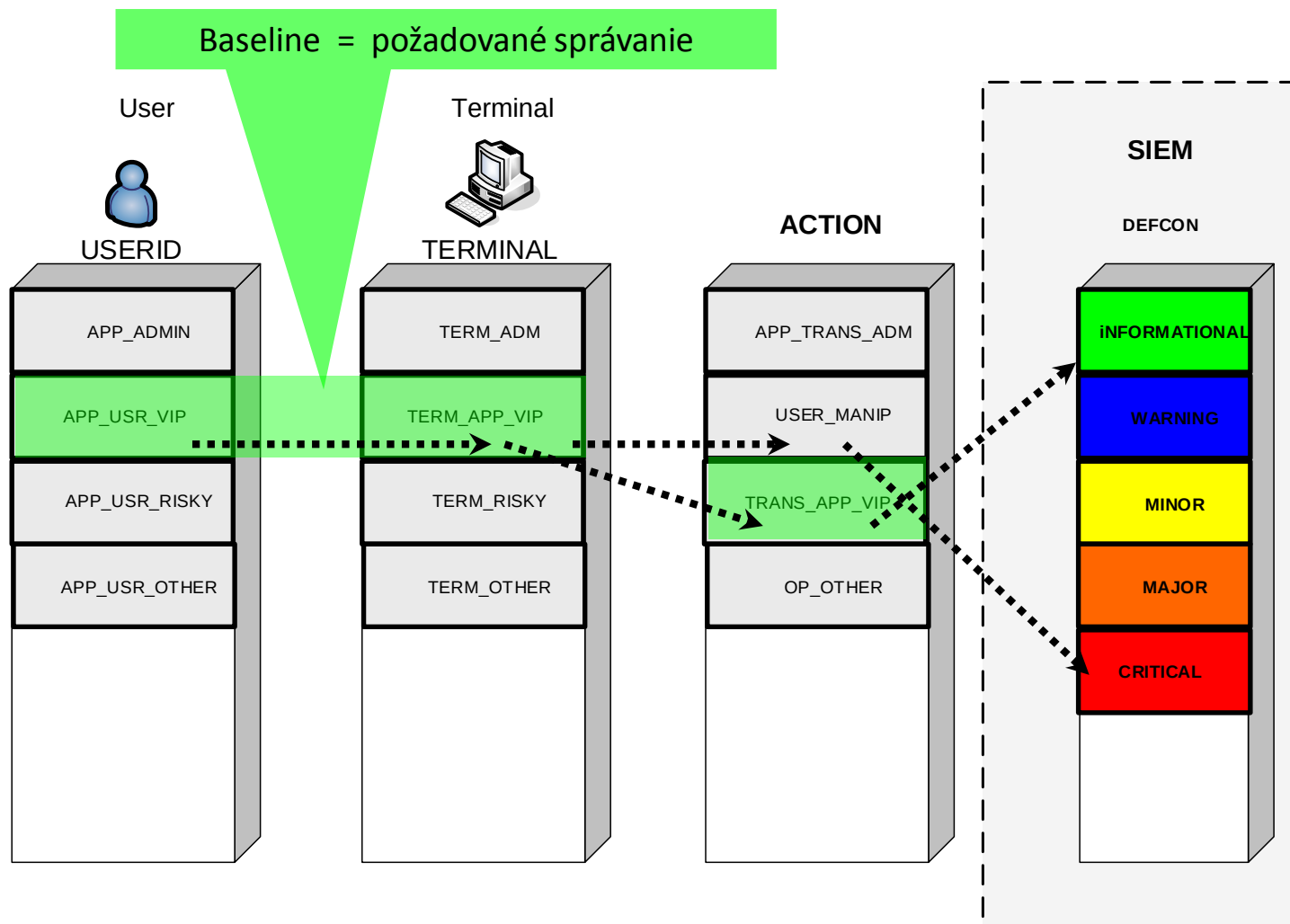
- Maximum nezávislých zdrojov informácií integrovaných do SIEM
- Cieľavedomé umiestnenie zdrojov informácií a ich vyladenie
- Online dostupnosť historických dát
 - existencia záznamov aj o 'bežných' aktivitách
 - možnosť rýchleho dohľadania záznamov o činnosti
- Flexibilné analytické nástroje
 - rýchla zmena focusu
 - vyhľadávanie súvislostí

Integrácia aplikácií do SIEM

- Klasické zdroje nepostačujú => **integrujme logy aplikácií**
 - dôraz na **bezpečnostné aspekty** hlásení aplikácií
 - výhoda **jednotnej vyšetrovacej konzoly**, jednotného pohľadu a silných analytických nástrojov
 - **automatická korelácia** hlásení aplikácie s hláseniami NIDS, firewallov, AV, HIPS, OS a ďalších
- Ako vyšetrovať logy z aplikácie ?
 - middleware - **Policy Compliance Engine**
 - **predspracovanie** hlásení pre SIEM - odľahčenie SIEM
 - **baseline-model** popisujúci požadovaný stav
 - real-time porovnávanie každého hlásenia s baseline a reporting odchýlok

PCE – compliance checking

Princíp baseline



LYNX- implementácie SIEM

- **Sektory:**
Telco, Banky, Utilities , Ministerstvo obrany SR, Ministerstvo zdravotníctva, Ministerstvo Financí
- **Doplnenie unikátnych črt:**
insider detection
fraud risk detection
monitorovanie prístupu k citlivým údajom
integrácia IDM
upravovanie štandardných agentov pre skvalitnenie monitorovania
- **Integrácia proprietárnych aplikácií (viac ako 20):**
Document management, CRM, DataWarehouse, billing, core banking, SAP, ..

Ďakujem za pozornosť

eFOCUS

